

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-140302

(43)Date of publication of application : 17.05.2002

(51)Int.Cl.

G06F 15/00

H04L 9/32

(21)Application number : 2000-331353

(71)Applicant : HORINAOKI

(22)Date of filing : 30.10.2000

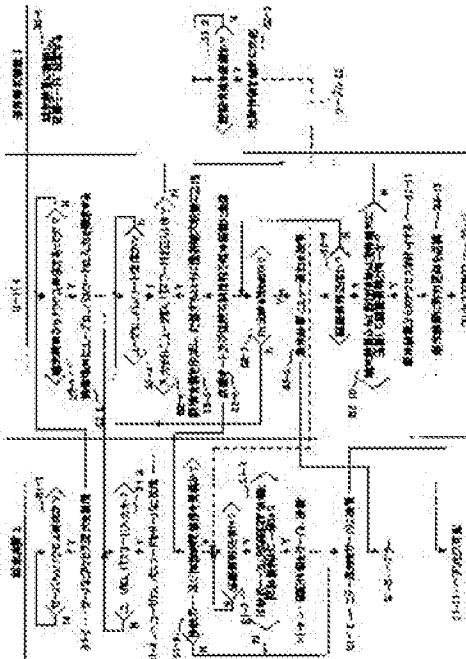
(72)Inventor : HORINAOKI

## (54) METHOD AND DEVICE FOR AUTHENTICATION AND TERMINAL DEVICE

### (57)Abstract:

**PROBLEM TO BE SOLVED:** To provide a method and a device for authentication and a terminal device which disable a multi-user computer system and a network system to illegally be used with ease when a method and a device for authentication and a terminal for identification when they are used.

**SOLUTION:** The authenticating device (4) sends prescribed information to a previously registered 2nd terminal device (3) at an authentication request from a 1st terminal device (2), the 2nd terminal device (3) sends the prescribed information to the 1st terminal device (2), and the specific information from the 2nd terminal device (3) is sent back from the 1st terminal device (2) to the authenticating device; and the authenticating device (4) compares the information sent back from the 1st terminal device (2) with the information sent out to the 2nd terminal device (3) and judges the adequacy of the 1st terminal device (3) according to the comparison result.



(19) 日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号  
特開2002-140302  
(P2002-140302A)

(43)公開日 平成14年5月17日(2002.5.17)

(51) Int.Cl.<sup>7</sup> 識別記号 F I テーマト<sup>8</sup>(参考)  
 G 0 6 F 15/00 3 3 0 G 0 6 F 15/00 3 3 0 C 5 B 0 8 6  
 H 0 4 L 9/32 H 0 4 L 9/00 6 7 3 A 5 J 1 0 4

審査請求 未請求 請求項の数 7 OL (全 14 頁)

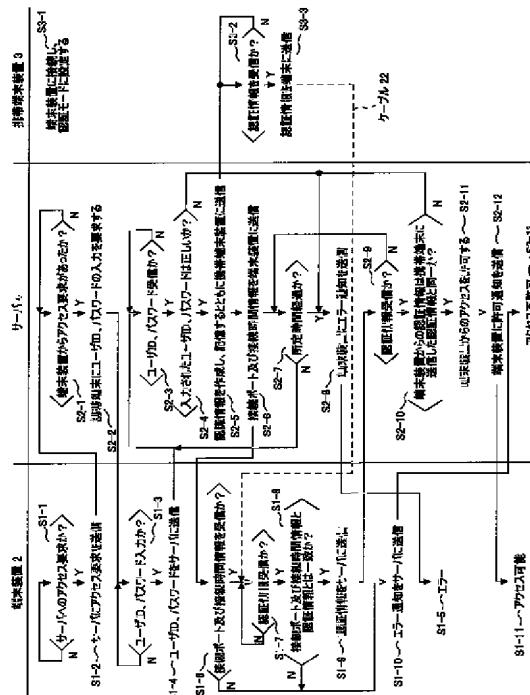
(21)出願番号	特願2000-331353(P2000-331353)	(71)出願人	500503780 堀 直樹 北海道札幌市西区福井 8 丁目 3 - 6
(22)出願日	平成12年10月30日(2000.10.30)	(72)発明者	堀 直樹 北海道札幌市西区福井 8 丁目 3 - 6
(74)代理人	100070150 弁理士 伊東 忠彦 F ターム(参考) 5B085 AE04 AE23 5J104 AA07 KA01 KA02 KA20 NA05 PA02 PA07		

(54) 【発明の名称】 認証方法及び認証装置並びに端末装置

(57) 【要約】

**【課題】** マルチユーザのコンピュータ・システムやネットワーク・システムを使用する際に本人であることを確認するための認証方法及び認証装置並びに端末装置に關し、不正利用を容易に行なえない認証方法及び認証装置並びに端末装置を提供することを目的とする。

【解決手段】 認証装置（4）から、第1の端末装置（2）からの認証要求に応じて予め登録された第2の端末装置（3）に所定の情報を送出し、前記第2の端末装置（3）から前記第1の端末装置（2）に前記所定の情報を送出し、前記第2の端末装置（3）からの前記所定の情報を前記第1の端末装置（2）から前記認証装置に返送し、前記認証装置（4）で、前記第1の端末装置（2）から返送される情報と前記第2の端末装置（3）に送出した前記所定の情報を比較して、その比較結果に基づいて前記第1の端末装置（3）の正当性を判定する。



**【特許請求の範囲】**

【請求項1】 認証装置から、第1の端末装置からの認証要求に応じて予め登録された第2の端末装置に所定の情報を送出し、

前記第2の端末装置から前記第1の端末装置に前記所定の情報を送出し、

前記第2の端末装置からの前記所定の情報を前記第1の端末装置から前記認証装置に返送し、

前記認証装置で、前記第1の端末装置から返送される情報と前記第2の端末装置に送出した前記所定の情報を比較して、その比較結果に基づいて前記第1の端末装置の正当性を判定することを特徴とする認証方法。

【請求項2】 前記第2の端末装置は、現在位置情報を検出し、前記第2の端末装置から前記第1の端末装置に送出する情報に該位置情報を合成して前記第1の端末装置に送出し、

前記認証装置は、前記第1の端末装置から返送される位置情報を、予め登録された位置情報を比較して、その比較結果に基づいて前記第1の端末装置の正当性を判定することを特徴とする請求項1記載の認証方法。

【請求項3】 第1の端末装置から認証が要求された場合、該第1の端末装置からの認証要求に応じて予め登録された第2の端末装置に所定の情報を送信し、

前記第1の端末装置からの返送情報を前記第2の端末装置への前記所定の情報を比較し、

前記第1の端末装置からの前記返送情報を前記第2の端末装置への前記所定の情報をで所定の対応がとれたときに、前記第1の端末装置を正当であると判定する認証処理部を有することを特徴とする認証装置。

【請求項4】 前記第2の端末装置は、現在位置を検出し、前記第1の端末装置への情報を合成して前記第1の端末装置に送出し、

前記認証処理部は、予め登録された位置情報を、前記第2の端末装置で合成された位置情報を比較し、両位置情報の対応がとれたときに、前記第1の端末装置を正当であると判定することを特徴とする請求項3記載の認証装置。

【請求項5】 認証処理状態を設定する設定部と、前記設定部により認証処理状態が設定された場合に、認証装置から情報を受信したとき、該認証装置からの情報を他の端末装置に送信する認証処理部を有することを特徴とする端末装置。

【請求項6】 現在位置を示す位置情報を検出する検出部を有し、

前記認証処理部は、前記認証装置からの情報に前記検出部で検出された前記位置情報を付加して前記他の端末装置に送信することを特徴とする請求項5記載の端末装置。

【請求項7】 認証要求時に、他の端末装置から供給される情報を受信し、

前記他の端末装置からの情報を、手動又は自動で認証装置に送信する認証処理部を有することを特徴とする端末装置。

**【発明の詳細な説明】****【0001】**

【発明の属する技術分野】本発明は認証方法及び認証装置並びに端末装置に係り、特に、マルチユーザのコンピュータ・システムやネットワーク・システムを使用する際に本人であることを確認するための認証方法及び認証装置並びに端末装置に関する。

【0002】近年、インターネット上でショッピングなどの商取引を行うことができるようになっており、その取引の代金支払いのための手続きにも認証処理が不可欠になっている。このため、安全確実な認証方式が求められている。

**【0003】**

【従来の技術】マルチユーザのコンピュータ・システムやネットワーク・システムで個人を認証する際には、通常ユーザーIDとパスワードの組み合わせによって認証が行われる。

【0004】例えば、ユーザがコンピュータ・システムやネットワークにログ・インする際に、ユーザーIDとパスワードの入力が要求される。ユーザが両方のデータを入力すると、それがあらかじめアクセス許可リストに登録されたものかどうかの認証が行なわれ、認証された場合にシステムの使用が許可される。

**【0005】**

【発明が解決しようとする課題】しかるに、従来の認証システムは、通常ユーザーIDとパスワードによってシステムの使用が許可されるため、第三者にユーザーIDとパスワードとが知られた場合には、第三者がユーザーIDとパスワードの取得者のユーザになりますましてシステムを使用することができる。このため、第三者に電子メールの内容をのぞかれたり、電子メールの送受信の履歴が見られて、だれとメールのやり取りしているのかなどの情報を知られたりしてしまう。また、第三者により勝手にインターネットやパソコン通信が使用され、覚えのない利用料金を請求されたり、覚えのない物品購入、販売や詐欺行為など不正利用されたりするなどの問題点があった。

【0006】本発明は上記の点に鑑みてなされたもので、不正利用を容易に行なえない認証方法及び認証装置並びに端末装置を提供することを目的とする。

**【0007】****【課題を解決するための手段】**

本発明は、認証装置(4)から、第1の端末装置(2)からの認証要求に応じて予め登録された第2の端末装置(3)に所定の情報を送出し、前記第2の端末装置(3)から前記第1の端末装置(2)に前記所定の情報を送出し、前記第2の端末装置(3)からの前記所定の情報を前記第1の端末装置

置(2)から前記認証装置に返送し、前記認証装置(4)で、前記第1の端末装置(2)から返送される情報と前記第2の端末装置(3)に送出した前記所定の情報とを比較して、その比較結果に基づいて前記第1の端末装置(3)の正当性を判定するものである。

【0008】本発明によれば、ユーザIDやパスワードを知っているだけでは第1の端末装置(2)は認証されることなく、第1の端末装置(2)と第2の端末装置(3)とを組み合わせて使用する必要があるため、ユーザIDやパスワードの不正使用が困難になる。

【0009】また、本発明は、前記第2の端末装置(3)で現在位置を検出し、前記第2の端末装置(3)から前記第1の端末装置(2)に送出する情報に前記位置情報を合成して前記第1の端末装置(2)に送出し、前記認証装置(4)で、前記第1の端末装置(2)から返送される前記位置情報と、予め登録された位置情報とを比較して、その比較結果に基づいて前記第1の端末装置(2)の正当性を判定するようにしてなる。

【0010】本発明によれば、第2の端末装置(3)が認証装置(4)に予め登録された位置に対応する位置にあるときに、第1の端末装置(2)の正当性が判定されるので、ユーザIDやパスワードの不正使用をさらに困難にできる。

#### 【0011】

【発明の実施の形態】図1に本発明の第1実施例のシステム構成図を示す。

【0012】本実施例のシステム1は、端末装置2、携帯端末装置3、サーバ4、ネットワーク5を含む構成とされている。

【0013】端末装置2は、例えば、パーソナルコンピュータやゲーム機などから構成されており、ネットワーク5を介してサーバ4にアクセス可能とされている。

【0014】図2に本発明の第1実施例の端末装置にプロック構成図を示す。

【0015】端末装置2は、CPU11、RAM12、ROM13、ハードディスクドライブ14、CD-ROMドライブ15、入力装置16、表示装置17、表示コントローラ18、インターフェースコントローラ19、モデム20を含む構成とされている。CPU11は、サーバ4へのアクセス時にハードディスクドライブ14に予めインストールされた認証用プログラムに基づいて認証処理を行なう。RAM12は、CPU11での処理を実行する際の作業用記憶領域として用いられる。

【0016】CPU11で実行される認証用プログラムは、例えば、CD-ROM21に書き込まれてユーザに提供され、CD-ROMドライブ14によりハードディスクドライブ14にインストールされる。なお、本実施例では、認証用プログラムをCD-ROM21により提供するようにしたが、フロッピー(登録商標)ディスク、光磁気ディスク、他の光ディスクなど他の記録媒体

で提供するようにもよい。また、所定のサーバからネットワークを介して提供するようにしてもよい。

【0017】インターフェースコントローラ19は、携帯端末装置3にケーブル22を介して接続され、携帯端末装置3との通信制御を行ない、認証処理時には、携帯端末装置3から認証情報が供給される。モデム20は、ネットワーク5との通信制御を行うものであり、サーバ4にアクセス要求を送信するとともに、認証処理時にはサーバ4に認証情報を送信する。インターフェースコントローラ19は、携帯端末装置3にケーブル22を介して接続され、携帯端末装置3との通信制御を行なうものであり、認証処理時には、携帯端末装置3から認証情報が供給される。

【0018】なお、ROM13には、BIOS(Basic Input/Output System)が記憶されている。また、表示装置17は、表示コントローラ18により制御され、文字やグラフィックスなどの表示を行なう。

【0019】携帯端末装置3は、携帯電話機やPHS(Personal Handy Phone System)電話機などから構成されており、認証モード設定時にはサーバ4からネットワーク5を介して認証情報を受信し、受信した認証情報をケーブル22を介して端末装置2に認証情報を送信する。

【0020】図3に本発明の第1実施例の携帯端末装置のプロック構成図を示す。

【0021】携帯端末装置3は、アンテナ31、受信部32、送信部33、データ処理部34、インターフェースコントローラ35、マイクロフォン36、スピーカ37、操作部38を含む構成とされている。

【0022】アンテナ31で受信された受信信号は、受信部32に供給され、元のデータに復調される。受信部32で復調されたデータは、データ処理部34に供給される。データ処理部34は、メモリ34aを内蔵しており、このメモリ34aには認証プログラムが予め記憶されている。

【0023】データ処理部34は、操作部38の操作により、認証モードに設定されると、認証プログラムを実行する。データ処理部34で実行される認証プログラムは、サーバ4からの認証情報をインターフェースコントローラ35、ケーブル22を介して端末装置2に送信する処理が実行される。また、データ処理部34は、携帯電話機としての処理を実行する。

【0024】サーバ4は、端末装置2からのアクセス要求に応じて認証処理を実行し、アクセス要求があった端末装置2が認証されたときに、端末装置2に各種サービスを提供する。

【0025】次に、サーバ4の構成を説明する。

【0026】図4に本発明の第1実施例のサーバのプロック構成図を示す。

【0027】サーバ4は、CPU51、RAM52、R

OM53、ハードディスクドライブ54、CD-ROMドライブ55、入力装置56、表示装置57、表示コントローラ58、通信コントローラ59、認証情報データベース60を含む構成とされている。CPU51は、端末装置2からのアクセス時にハードディスクドライブ54に予めインストールされた認証プログラムに基づいて認証処理を行なう。RAM52は、CPU51での処理を実行する際の作業用記憶領域として用いられる。

【0028】認証プログラムは、例えば、CD-ROM63に書き込まれてユーザに提供され、CD-ROMドライブ54によりハードディスクドライブ54にインストールされてCPU51により実行される。なお、本実施例では、認証用プログラムをCD-ROM63により提供するようにしたが、フロッピーディスク、光磁気ディスク、他の光ディスクなど他の記録媒体で提供するようにもよい。また、サーバからネットワーク5を介して提供するようにしてもよい。

【0029】通信コントローラ59は、ネットワーク5との通信制御を行うものであり、端末装置2からのアクセス要求を受信するとともに、認証処理時には携帯端末装置3に認証情報を送信する。

【0030】認証情報データベース60には、少なくともアクセス元ID(Identification)情報61、送信先情報62が予め記憶されている。アクセス元ID情報61は、ユーザを識別するための識別情報である。送信先情報62は、認証情報を送信すべき先の情報であり、例えば、携帯端末装置3の電話番号である。

【0031】認証処理時には、認証情報データベース60に予め記憶された上記アクセス元ID情報61、送信先情報62に基づいて認証処理が実行される。

【0032】なお、ROM53には、BIOS(Basic Input/Output System)が記憶されている。また、表示装置57は、表示コントローラ58により制御され、文字やグラフィックスなどの表示を行なう。

【0033】次に本実施例の認証処理について説明する。

【0034】図5に本発明の第1実施例の認証処理の動作説明図を示す。

【0035】端末装置2でステップS1-1でサーバ4にアクセス要求するための操作が行なわれると、端末装置2は、ステップS1-2でネットワーク5のうち図1に実線で示す第1の通信経路を介してサーバ4にアクセス要求を送信する。このとき、第1の通信経路は、例えば、一般電話回線網である。

【0036】サーバ4は、ステップS2-1で端末装置2からアクセス要求を受信すると、ステップS2-2で第1の通信経路を介して端末装置2にユーザID、及び、パスワードの入力を要求する。

【0037】端末装置2は、ステップS1-3でサーバ4からのユーザID、及び、パスワードの入力の要求を

受信すると、ユーザID及びパスワードが手動又は自動で生成され、ステップS1-4でネットワーク5を介してサーバ4に送信される。

【0038】サーバ4は、ステップS2-3でユーザID及びパスワードを受信すると、ステップS2-4で受信したユーザID及びパスワードが予め登録されたものと一致するか否かを判定する。ステップS2-4で端末装置2から供給されたユーザID及びパスワードがサーバ4に予め登録されたユーザID及びパスワードと一致すれば、入力されたユーザID及びパスワードは正しいと判定されて、ステップS2-5で認証情報を作成する。

【0039】認証情報は、サーバ4で任意に作成されるキーワードとサーバ4の端末装置2が接続されているポート情報と接続された時間とを合成したものである。なお、ポート情報は、例えばサーバ4のIPアドレスであり、特定のサーバで認証が行なわれたことが証明できるものであればよい。また、ここでは、認証情報をポート情報及び接続時間情報を合成して作成しているが、これに限定されるものではなく、端末装置2からの接続を個別に識別できるものであればよい。

【0040】作成された認証情報は、ステップS2-5で、サーバ4内に記憶されるとともに、認証データベース60の送信先として登録された携帯端末装置3に送信される。さらに、ステップS2-6で認証情報のうちポート情報及び接続時間情報を端末装置2に通知する。

【0041】このとき、サーバ4と携帯端末装置3との通信は、図1に実線で示す端末装置2とサーバ4との第1の通信経路とは異なる図1に破線で示す第2の通信経路を介して行なわれる。例えば、携帯端末装置3とサーバ4とは、移動通信網を介して通信が行なわれ、端末装置2とサーバ4とは、インターネットと一般回線網を介して通信が行なわれる。なお、サーバ4と携帯端末装置3との通信は、端末装置2とサーバ4との通信とは同じ系統のネットワーク、例えば、一般回線網を用いたとしても一般回線網のうちで通信経路が異なればよい。

【0042】なお、サーバ4は、ステップS2-7で所定時間、端末装置2からユーザID及びパスワードが供給されないと判定した場合には、ステップS2-8で端末装置2にエラー通知を行なう。端末装置2は、ステップS1-5でサーバ4からエラー通知を受信すると、サーバ4へのアクセスはエラーとされる。

【0043】なお、携帯端末装置3は、ステップS3-1で、ケーブル22で端末装置4に接続されるとともに、認証モードとされている。携帯端末装置3は、ステップS3-2で、認証情報を受信すると、ステップS3-3で受信した認証情報を端末装置4にケーブル22を介して送信する。なお、端末装置2と携帯端末装置3との通信を赤外線通信あるは無線通信で行なう場合には、ケーブル22での接続は不要となる。

【0044】端末装置2は、ステップS1-6でサーバ4への接続時にサーバ4のポート情報を接続時間情報を受信しており、ステップS1-7で携帯端末装置3から認証情報を受信すると、ステップS1-8で携帯端末装置3から受信した認証情報と、サーバ4から受信した接続ポート番号情報及び接続時間情報を比較し、一致するか否かを判定する。ステップS1-8で認証情報とサーバ4から受信したポート情報を接続時間情報とが一致する場合には、ステップS1-9で認証情報をサーバ4にネットワーク5のうちの図1に実線で示す第1の通信経路を介して送信する。また、ステップS1-8で認証情報とサーバ4から受信した接続ポート番号情報及び接続時間情報とが不一致の場合には、ステップS1-10でサーバ4にエラー通知が送信され、認証処理は中断される。また、ステップS1-6でサーバ4からポート番号情報及び接続時間情報を受信できない場合にもステップS1-10でサーバ4にエラー通知が送信される。なお、サーバ4は、ステップS2-13で端末装置2からエラー通知を受信すると、端末装置2からのアクセスを不許可する。このように、端末装置2側で接続ポート番号情報及び接続時間情報を受信し、携帯端末装置3から供給された認証情報を比較することによりユーザ側でサーバ4の認証を行なえる。このため、悪質なサーバからの保護を行なうことができる。

【0045】サーバ4は、ステップS2-9で端末装置2から認証情報を受信すると、ステップS2-10で端末装置2から受信した認証情報をステップS2-5で携帯端末装置3に送信した認証情報を比較し、一致するか否かを判定する。ステップS2-10で、認証情報が一致した場合には、携帯端末装置3と端末装置2とがケーブル22により接続されていると判定でき、携帯端末装置3の所有者であるユーザが端末装置2からサーバ4にアクセスを要求していると判定できるため、ステップS2-11で端末装置2にアクセスを許可し、ステップS2-12で端末装置2にアクセス許可通知を送信する。

【0046】端末装置2は、ステップS1-11でサーバ4からアクセス許可通知を受信すると、サーバ4にアクセスしてサービスを享受することができる。

【0047】本実施例によれば、ユーザID及びパスワードを知っているだけではサーバ4にアクセスできず、アクセスするためには携帯端末装置3が必要となる。よって、第三者が他人のユーザID及びパスワードを使ってサーバ4にアクセスすることを防止できる。

【0048】なお、本実施例では、端末装置2と携帯端末装置3とのデータ通信をケーブル22により行なっているが、IrDA方式などの赤外線通信や無線通信によりデータ通信を行なうようにしてもよい。

【0049】また、本実施例では、認証情報を端末装置2のサーバ4への接続ポート情報を並びに時刻情報を合成

して生成しているが、サーバ4に予めアクセスする位置情報を登録するとともに、携帯端末装置3に位置情報検出装置を内蔵し、携帯端末装置3から端末装置2を介して位置情報を送信し、位置情報の一一致を認証条件に付加することにより、認証を正確に行なえる。

【0050】図6に本発明の第2実施例のブロック構成図を示す。同図中、図1と同一構成部分には同一符号を付し、その説明は省略する。

【0051】本実施例のシステム100は、サーバ111の認証情報データベース112のデータ構成及び携帯端末装置113の構成が相違する。

【0052】認証情報データベース112のデータ構成は、図1に示す認証情報データベース60に位置情報114が付加された点で相違する。また、携帯端末装置113は、位置情報検出装置115を有する点で携帯端末装置2とは相違する。

【0053】位置情報検出装置115は、例えば、GPS (Global Positioning System) による測位装置から構成されている。位置情報検出装置115は、携帯端末装置113が認証モードのときに、GPS衛星121からの電波を受信することにより携帯端末装置113の位置を検出することが可能な構成とされている。位置情報検出装置115で検出された位置情報は、サーバ111から認証情報を受信したときに、受信した認証情報に附加される。

【0054】図7に本発明の第2実施例の認証処理の動作説明図を示す。同図中、図5と同一ステップには同一符号を付し、その説明は省略する。

【0055】本実施例の認証処理は、携帯端末装置113の処理にステップS3-11、S3-12を付加するとともに、サーバ111の処理にステップS2-21を付加してなる。ステップS3-11は、ステップS3-1で認証モードとされたときに、位置検出装置115により位置を検出するステップである。ステップS3-12は、ステップS3-2で携帯端末装置113にサーバ111から認証情報が受信されたときに、ステップS3-1で位置情報検出装置115により検出された位置情報をサーバ111からの認証情報に附加して端末装置2に送信するステップである。

【0056】ステップS2-21では、位置情報検出装置115で検出された位置情報と認証情報データベース112に予め登録された位置情報を比較し、位置情報検出装置115で検出された位置情報が認証情報データベース112に予め登録された位置情報を中心として所定の範囲内に存在するときには、正当であると判定し、位置情報検出装置115で検出された位置情報が認証情報データベース112に予め登録された位置情報を中心とした所定の範囲外のときには、正当でないと判定する。

【0057】ステップS2-21で位置が正当でないと

判定された場合には、ステップS2-7で端末装置2にエラーが通知され、端末装置2のサーバ111へのアクセスは拒否される。

【0058】本実施例によれば、携帯端末装置113及び端末装置2が認証情報データベース112に予め登録された位置情報を中心とした所定の範囲内にあるときに、サーバ111へのアクセスが承認される。このため、自宅など所定の場所でしかアクセスが許可されなくなる。よって、第三者が不正にアクセスしようとすると、ユーザの自宅に侵入する必要があるので、容易に不正アクセスを行うことはできない。

【0059】また、本実施例では、サーバ4が携帯端末装置112の位置情報を認識することができ、この位置情報を用いることによりSOHO (small office home office) にて勤務している者の 勤務状況の把握に有効となる。また、行政上の申請や届出の際の認証などにも有効となる。

【0060】なお、上記第1及び第2実施例では、パソコンによるサーバ4へのアクセスのための認証方式に本発明の認証方式を用いたが、クレジットカードの端末や自動販売機などの不正使用を防止するために本発明の認証方式を用いるようにしてもよい。

【0061】図8に本発明の第3実施例のブロック構成図、図9に本発明の第3実施例の動作説明図を示す。同図中、図1、図5と同一構成部分には同一符号を付し、その説明は省略する。

【0062】本実施例のシステム200は、買い物の支払いをクレジットカード201で行なう際に使用されるシステムである。本実施例のシステム200で使用されるクレジットカード読み取り装置202には、第1実施例の端末装置2に相当する機能が組み込まれている。

【0063】クレジットカード201で支払いを行なう場合に、携帯端末装置3をカード読み取り装置202にケーブル22により接続し、携帯端末装置3の動作モードを認証モードにする。カード読み取り装置202は、ステップS1-31でクレジットカード201が読み取られると、ネットワーク5のうち図8に実線で示す第1の通信経路を介してサーバ4にアクセス要求を行なう。

【0064】サーバ4は、カード読み取り装置202からアクセス要求があると、カード読み取り装置202に対してユーザID及びパスワードの入力を要求する。クレジットカード201の使用者によりユーザID及びパスワードの入力が行なわれると、カード読み取り装置202は、図8に実線で示す第1の通信経路を介してサーバ4にユーザID及びパスワードを送信する。

【0065】なお、ユーザID及びパスワードは入力するのではなくクレジットカードから提供されるようにしてもよい。

【0066】サーバ4は、カード読み取り装置202からネットワーク5のうち図8に実線で示す第1の通信経路を

介してアクセス要求があり、ユーザID及びパスワードが承認されると、第1実施例と同様に図8に破線で示す第2の通信経路を介して携帯端末装置3に認証情報を送信する。携帯端末装置3も第1実施例と同様に認証情報をカード読み取り装置202にケーブル22、赤外線通信、無線通信などにより送信する。

【0067】カード読み取り装置202は、携帯端末装置3から認証情報を受信すると、ネットワーク5のうち図8に実線で示す第1の通信経路を介してサーバ4に認証情報を送信する。サーバ4は、第1実施例と同様に端末装置2からの認証情報を携帯端末装置3に送信した認証情報と比較して、一致したときには、ステップS2-31で商品の代金に対応した金額を予め登録された口座から引き落とし、ステップS2-32でカード読み取り装置202に支払い完了通知を送信する。

【0068】カード読み取り装置202では、サーバ4から支払い完了通知を受信すると、ステップS1-12で支払いが完了した旨の通知を行なう。

【0069】本実施例によれば、ユーザID及びパスワード並びに携帯端末装置を所持したユーザだけがクレジットカード201を使用することができ、クレジットカード201の不正使用が困難となる。

【0070】図10に本発明の第4実施例のブロック構成図、図11に本発明の第4実施例の動作説明図を示す。同図中、図1、図5と同一構成部分には同一符号を付し、その説明は省略する。

【0071】本実施例のシステム300は、自動販売機301での支払いを行なう際に使用される認証システムである。本実施例のシステム300で使用される自動販売機301には、第1実施例の端末装置2に相当する機能が組み込まれている。

【0072】自動販売機301で支払いを行なう場合に、携帯端末装置3の動作モードを認証モードにする。自動販売機301は、ステップS1-41で商品が選択されると、サーバ4にアクセス要求を行なう。サーバ4は、自動販売機301からアクセス要求があると、自動販売機301に対してユーザID及びパスワードの入力を要求する。商品の購入者により自動販売機302に設けられたキーボード302によりユーザID及びパスワードの入力が行なわれると、自動販売機301は、サーバ4にユーザID及びパスワードを送信する。

【0073】なお、ユーザID及びパスワードは入力するのではなくカードなどにより提供されるようにしてもよい。

【0074】サーバ4は、自動販売機301からネットワーク5のうち図10に実線で示す第1の通信経路を介してユーザID及びパスワードが入力され、ユーザID及びパスワードが承認されると、第1実施例と同様に図10に破線で示す第2の通信経路を介して携帯端末装置3に認証情報を送信する。携帯端末装置3も第1実施例

と同様に認証情報を自動販売機301にケーブル22、赤外線通信、無線通信などにより送信する。

【0075】自動販売機301は、携帯端末装置3から認証情報を受信すると、ネットワーク5のうち図1に実線で示す第1の通信経路を介してサーバ4に認証情報を送信する。サーバ4は、第1実施例と同様に端末装置2からの認証情報を携帯端末装置3に送信した認証情報と比較して、一致したときには、ステップS2-31で商品の代金に対応した金額を予め登録された口座から引き落とし、ステップS2-32で自動販売機301に支払い完了通知を送信する。自動販売機301では、サーバ4から支払い完了通知を受信すると、ステップS1-42で商品を自動販売機301の取出口303より排出する。

【0076】本実施例によれば、ユーザID及びパスワード並びに携帯端末装置を所持したユーザだけが自動販売機301で商品入手することができ、不正使用が困難となる。また、自動販売機に現金を置く必要がないので、防犯上も好適となる。

【0077】なお、第1～第4実施例では、認証情報の送信先として携帯電話などの携帯端末装置3を例として説明したが、認証情報の送信先は、端末装置2とサーバ4との通信経路と異なっていればよく、通常の端末装置であってもよい。

【0078】なお、本発明の認証システムは、上記実施例に限定されるものではなく、本発明の請求の範囲を逸脱しない範囲で種々の変形例が可能である。

#### 【0079】

【発明の効果】上述の如く、本発明によれば、ユーザIDやパスワードを知っているだけでは第1の端末装置は認証されることはなく、第1の端末装置と第2の端末装置とを組み合わせて使用する必要があるため、ユーザIDやパスワードの不正使用が困難になるなどの特長を有

する。

【0080】本発明によれば、第2の端末装置で位置情報を附加することにより、第1の端末装置が認証装置に予め登録された位置に対応する位置にあるときに、第1の端末装置の正当性が判定されるので、ユーザIDやパスワードの不正使用をさらに困難にできるなどの特長を有する。

#### 【図面の簡単な説明】

【図1】本発明の第1実施例のシステム構成図である。

【図2】本発明の第1実施例の端末装置のブロック構成図である。

【図3】本発明の第1実施例の携帯端末装置のブロック構成図である。

【図4】本発明の第1実施例のサーバのブロック構成図である。

【図5】本発明の第1実施例の動作説明図である。

【図6】本発明の第2実施例のブロック構成図である。

【図7】本発明の第2実施例の動作説明図である。

【図8】本発明の第3実施例のブロック構成図である。

【図9】本発明の第3実施例の動作説明図である。

【図10】本発明の第4実施例のブロック構成図である。

【図11】本発明の第4実施例の動作説明図である。

#### 【符号の説明】

1, 100, 200, 300 認証システム

2 端末装置

3 携帯端末装置

4, 111 サーバ

5 ネットワーク

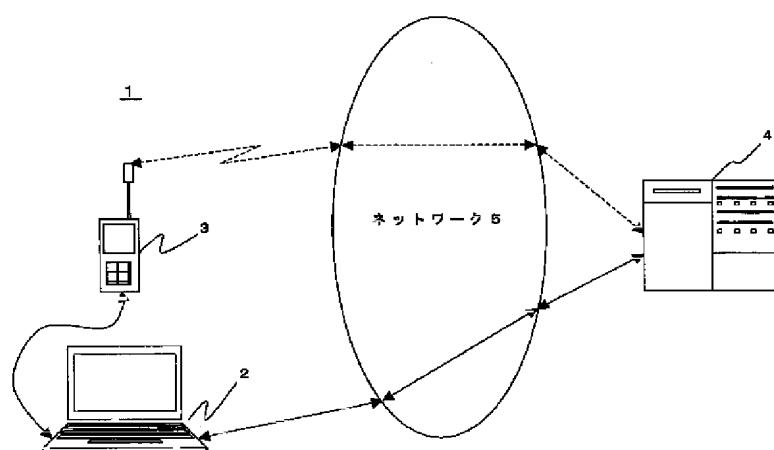
60, 112 認証情報データベース

61 アクセス元ID

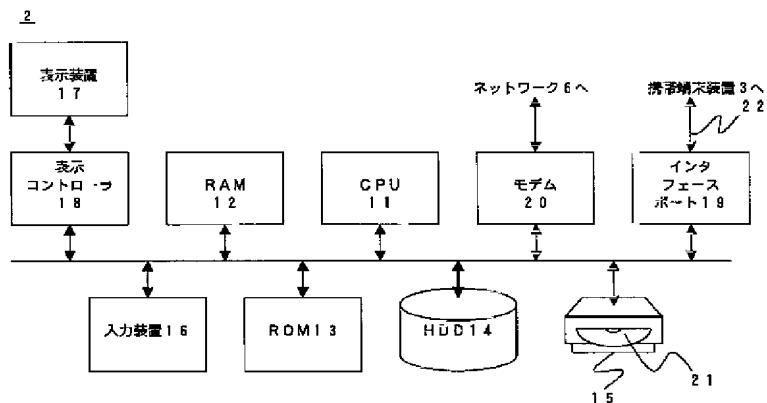
62 送信先情報

114 位置情報

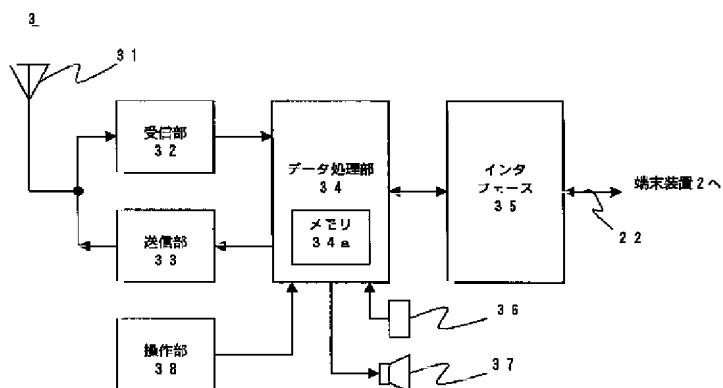
【図1】



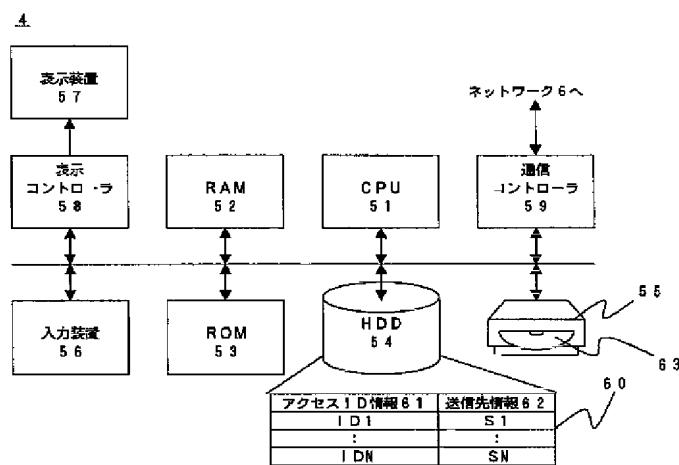
【図2】



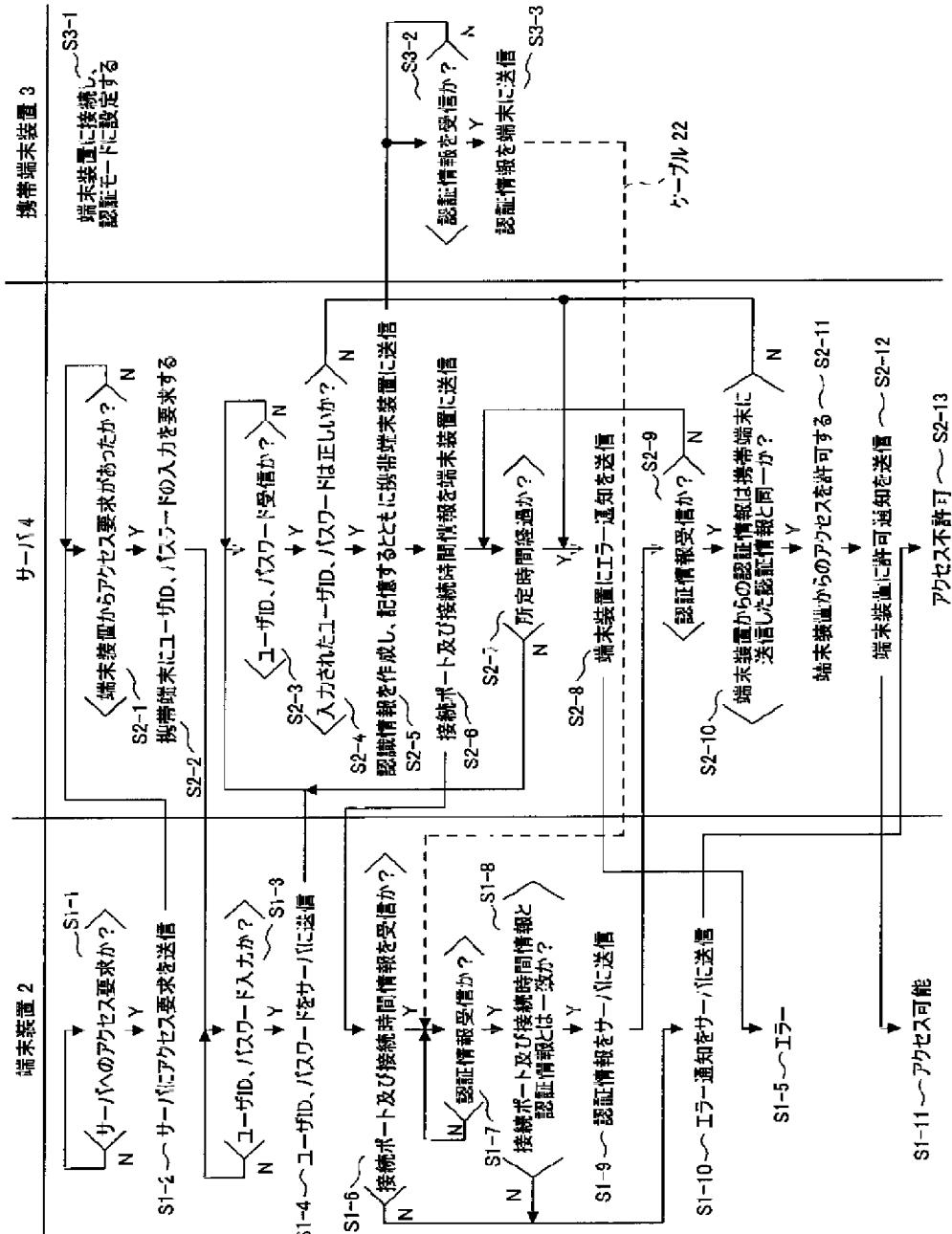
【図3】



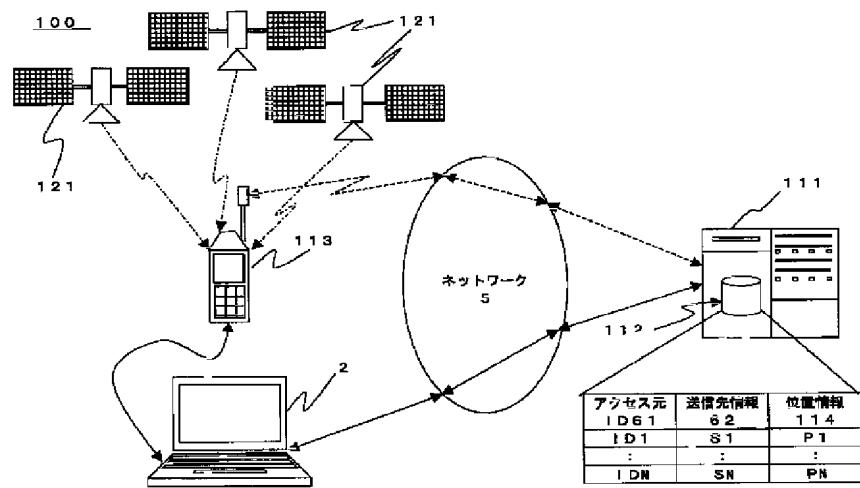
【図4】



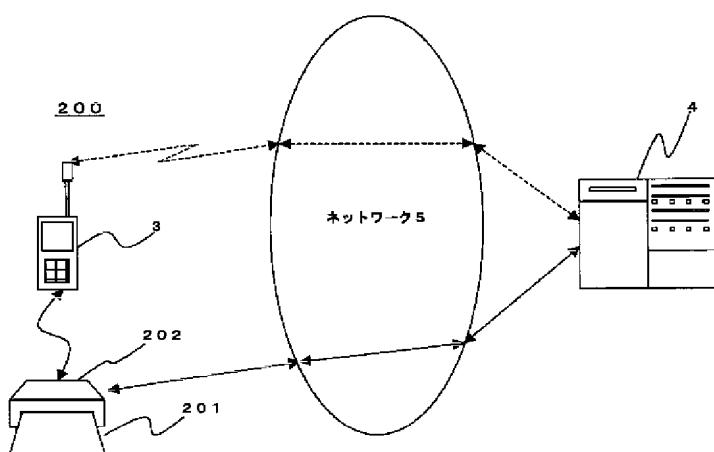
【図5】



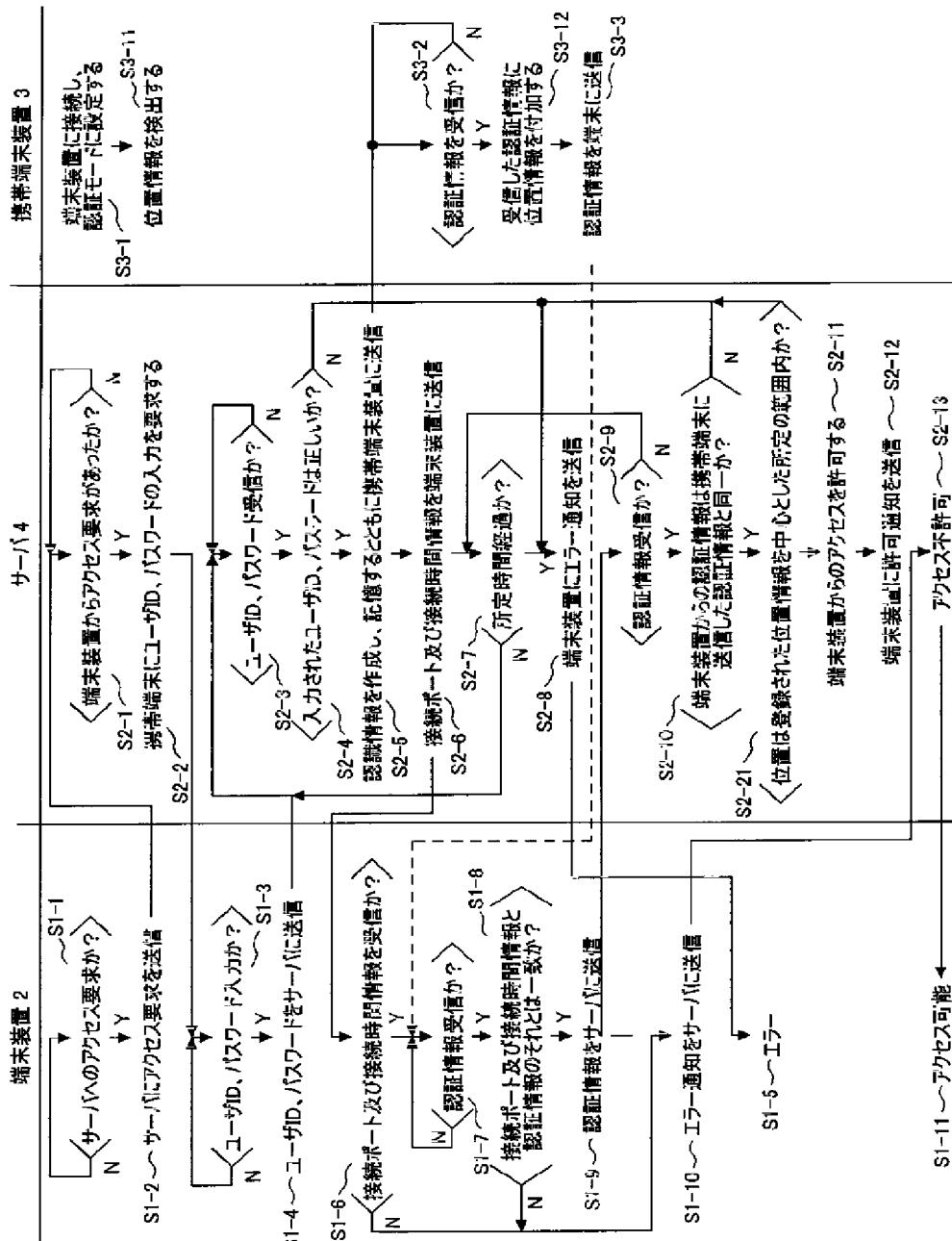
【図6】



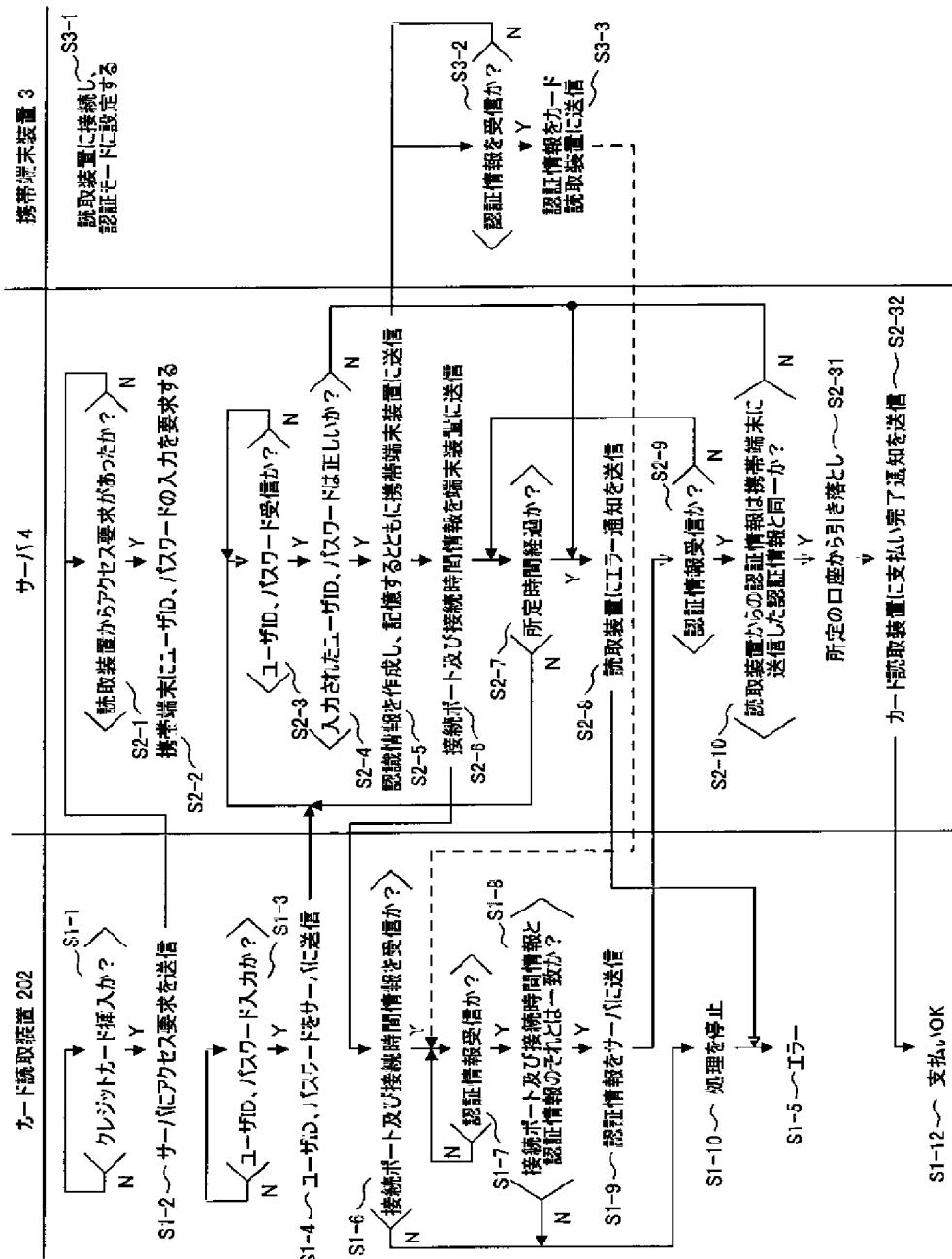
【図8】



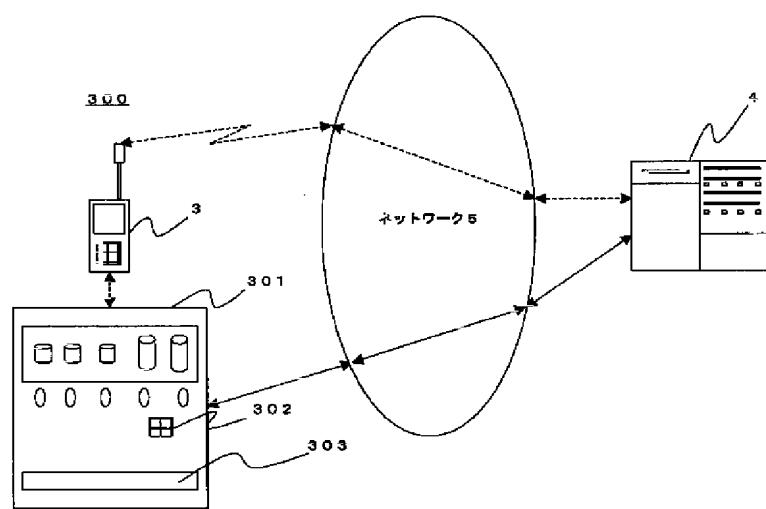
【図7】



【図9】



【図10】



【図11】

